Liveness Detection for Iris Recognition

Bori Toth
Deloitte & Touche LLP

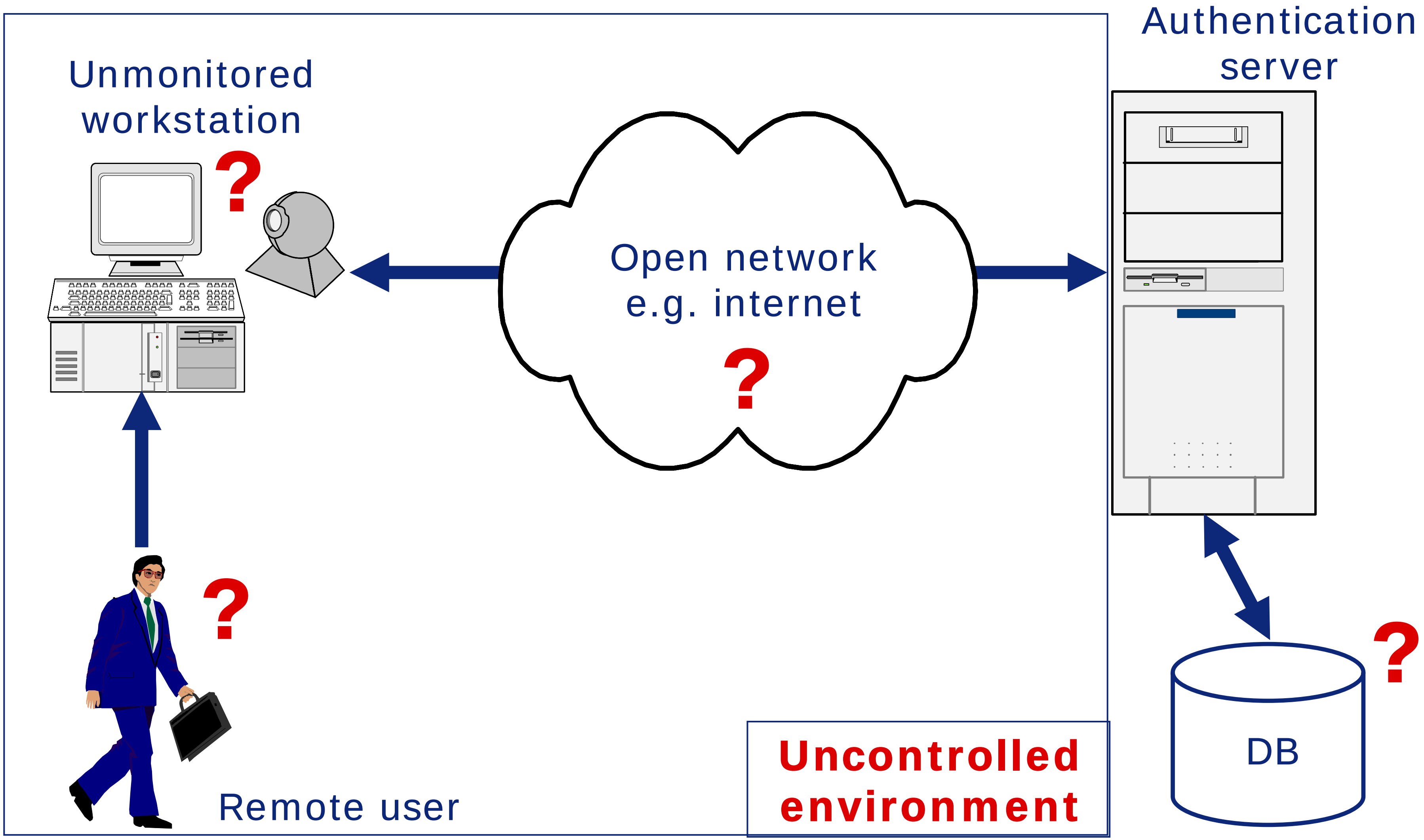
Ulf Cahn von Seelen, Ph.D.
Iridian Technologies Inc.

NIST Workshop
Biometrics and E-Authentication over Open Networks
30-31 March 2005, Gaithersburg (MD)

Agenda – Part 1

- Remote authentication scenario
- Iris recognition: threats
- Published spoofing attempts
- Risks
- Liveness detection methods

Remote authentication scenario



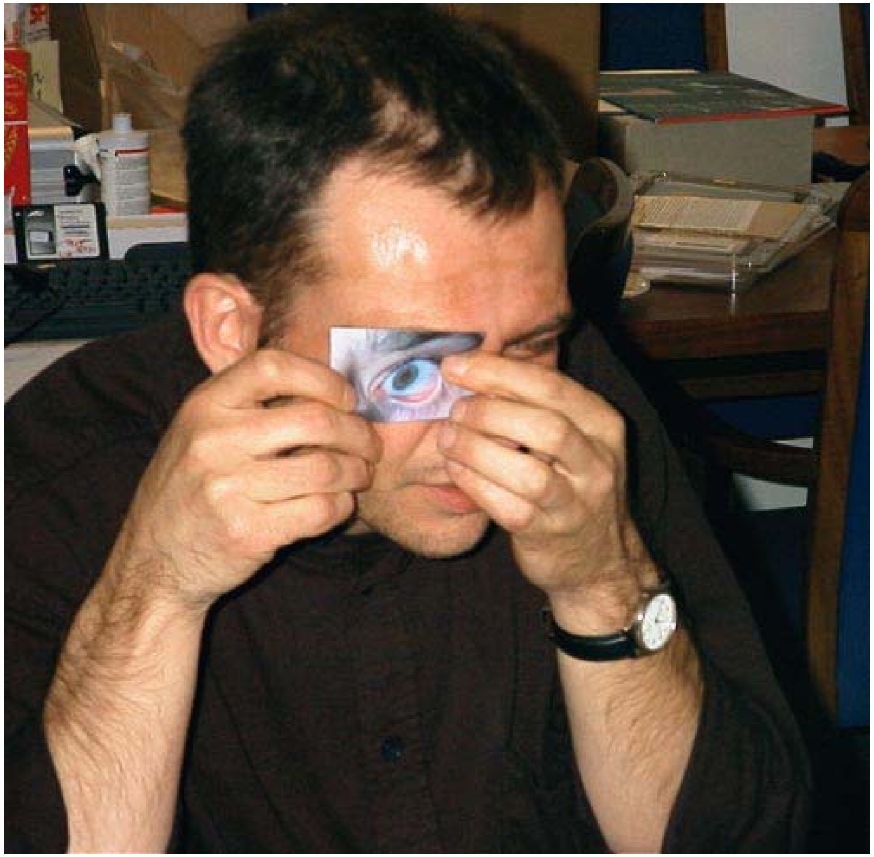
Deloitte.

Iris recognition: threats

- Eye image
  - Screen image
  - Photograph
  - Paper print
  - Video signal
- Artificial eye
  - Glass/plastic etc.
- Natural eye: impostor
  - Eye removed from body
  - Printed contact lens
- Natural eye: user
  - Forced use
- Capture/replay attacks
  - Eye image
  - IrisCode template

Published spoofing attempts

- C’t Magazine, 11/2002
  - Panasonic Authenticam BM-ET100
  - 2400 x 1200 dpi print with a hole for the pupil
  - Enrolment & verification



Published spoofing attempts

- Prof Matsumoto, Yokohama National University, 2004
  - Panasonic Authenticam BM-ET100
  - Oki IrisPass-WG (enrolment of printed iris image was not possible)
  - Oki IrisPass-h

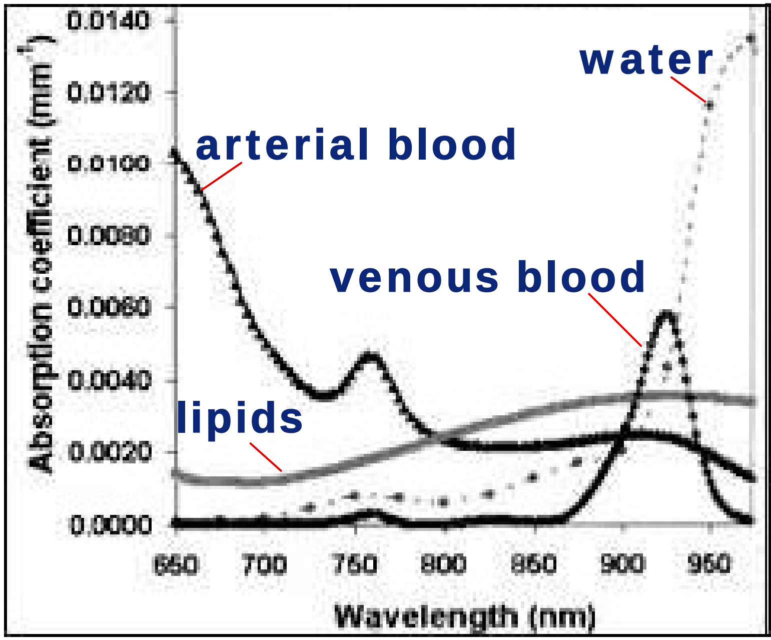
Risks

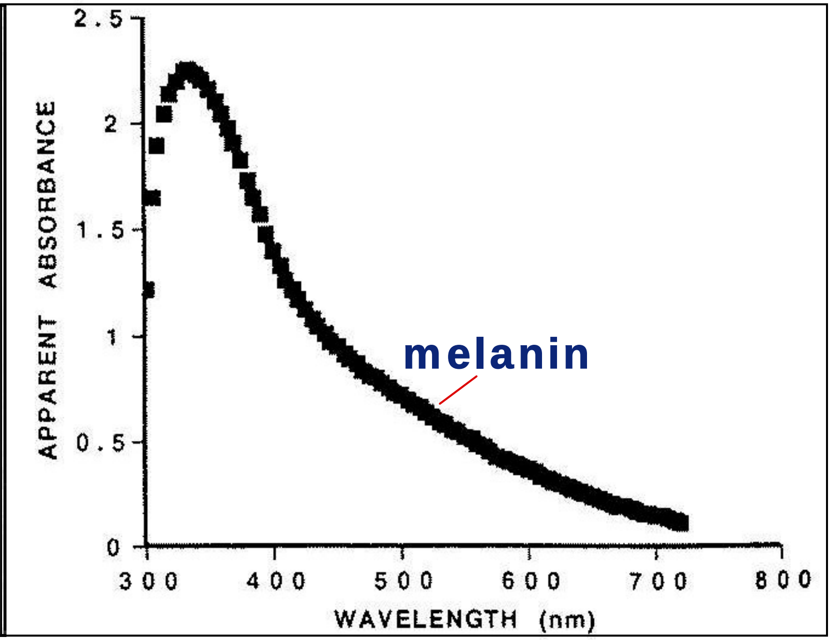
- Access list scenario
  - Assuming the rights/privileges of a legitimate user

- Watch list scenario
  - Not being recognized as a wanted person

Liveness detection methods

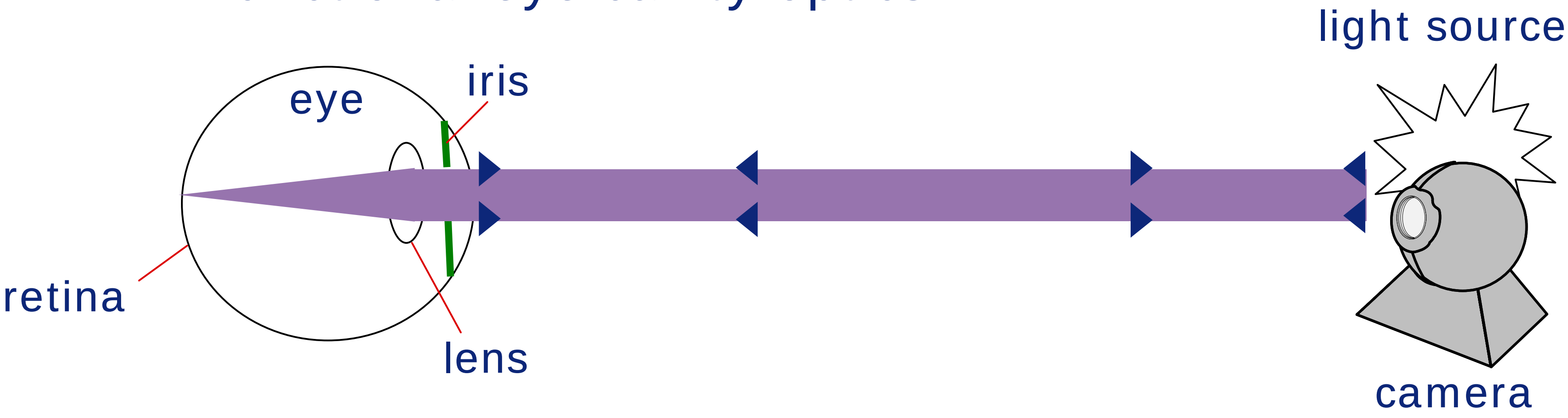
- Light absorbing properties of blood, fat, melanin
  - Living tissue?





Liveness detection methods

- Retinal light reflection: ‘red-eye’ effect
  - Functional eye cavity optics?

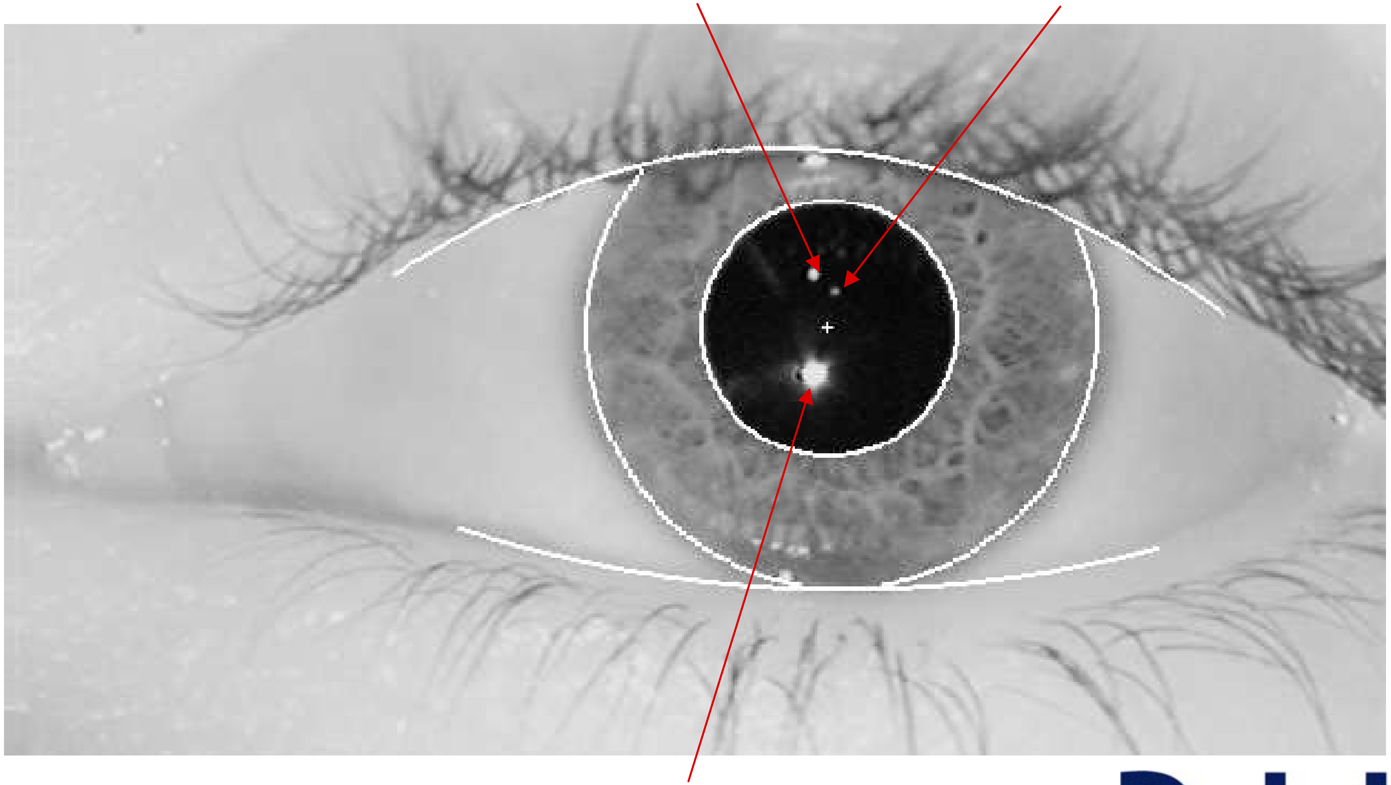


Light entering the eye is reflected back to the light source by the retina → functional human appears red because of the blood vessels behind the retina

Camera can capture this effect if it is close enough to the light source

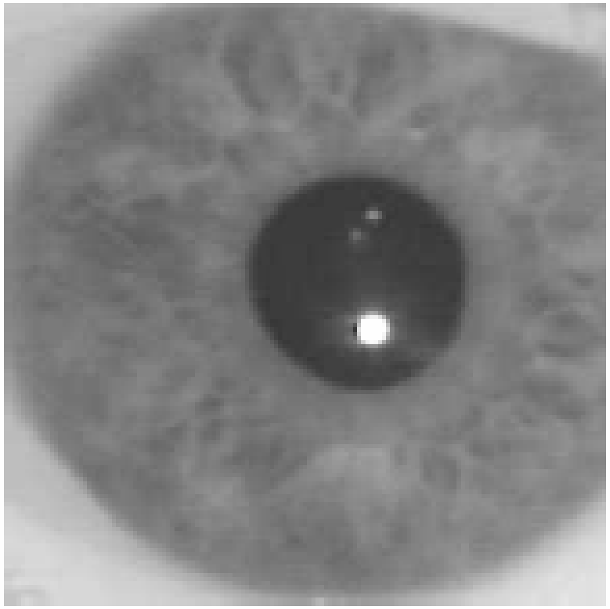
Liveness detection methods

- Purkinje reflections from cornea and lens
  - Natural eye: 4 optical surfaces reflect light
  - Position of light source → position of reflections

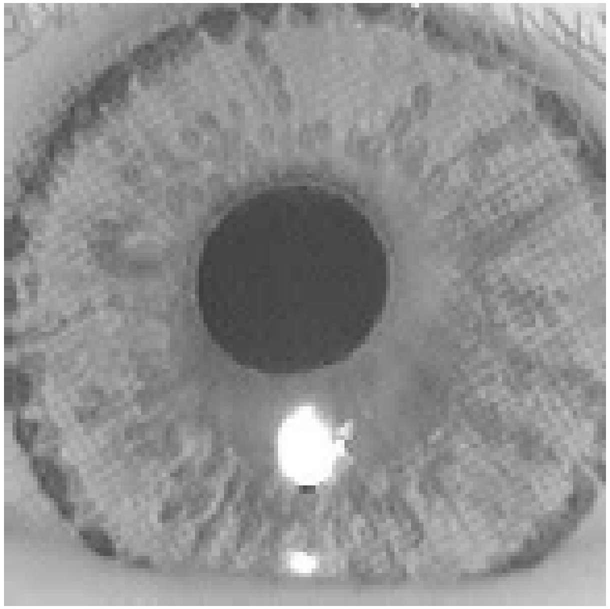


Liveness detection methods

- 2D Fourier detection of printing artefacts
  - Natural eye or printed lens?



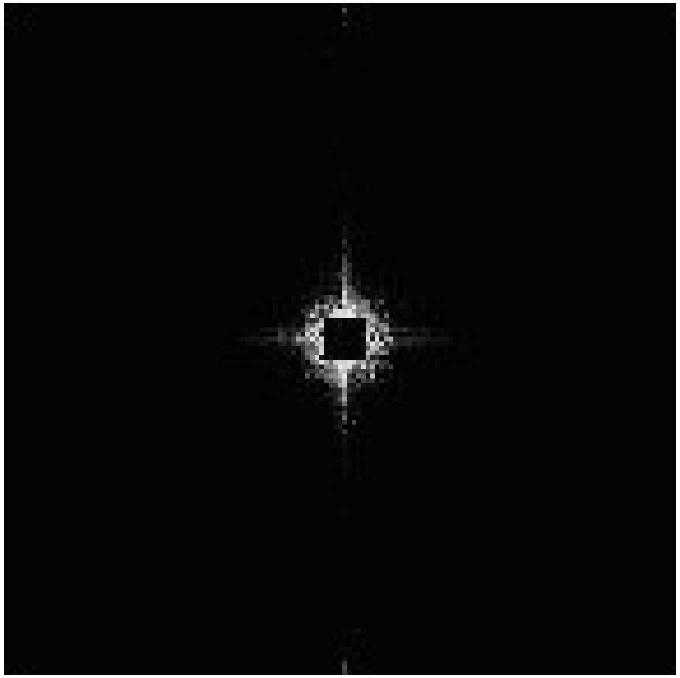
Natural iris



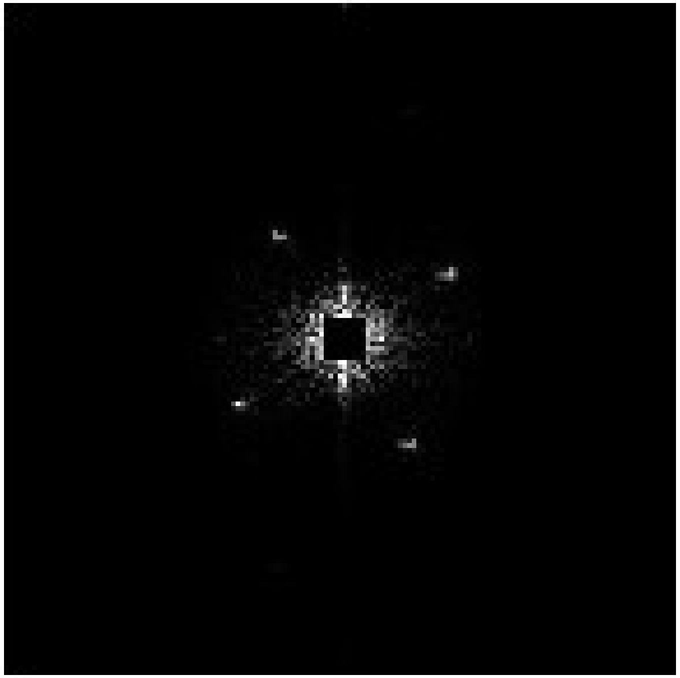
Fake iris printed on a contact lens

Liveness detection methods

- 2D Fourier detection of printing artefacts
  - Natural eye or printed contact lens?



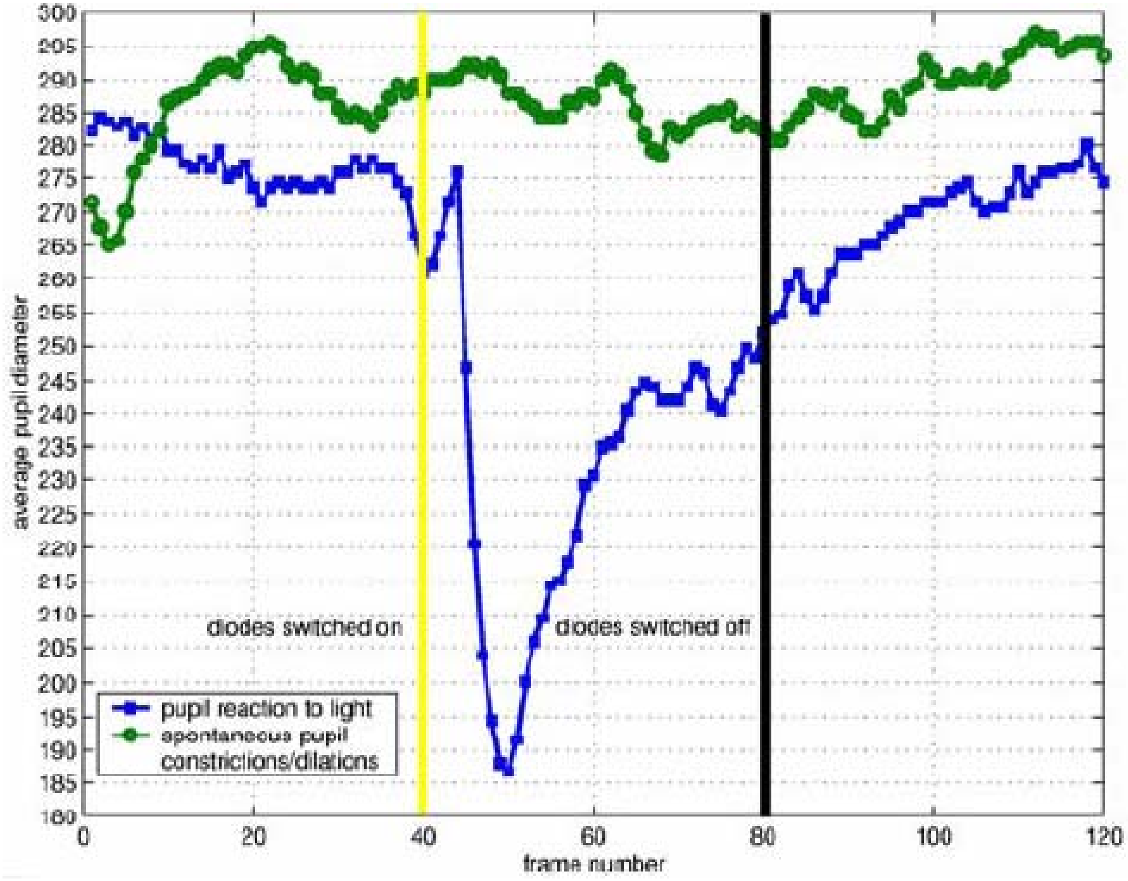
2D Fourier spectrum of natural iris



2D Fourier spectrum of fake iris printed on a contact lens

Liveness detection methods

- Behavioral countermeasures: involuntary
  - Pupillary unrest (hippus) & light reflex



Liveness detection methods

- Behavioral countermeasures: voluntary
  - Challenge-response: eyelid blinks, eye movements

- Methods beyond liveness testing
  - IrisCode byte scrambling: $256! = 10^{507}$ permutations

    ➡ Device-specific, session-specific, application-specific iris templates possible

  - Encryption of data (IrisCode or eye image) in transmission

  - IrisCode database protection

References

- Daugman (1999): Recognizing Persons by their Iris Patterns: Countermeasures against Subterfuge, in Jain et al. (eds.): Biometrics. Personal Identification in a Networked Society, pp. 103-121.
- Daugman (2004): Iris Recognition and Anti-Spoofing Countermeasures, at the 7th International Biometrics Conference, 2004, London. http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf
- Franceschini et al. (1999): Near-infrared Absorption and Scattering Spectra of tissues in vivo, in: Proceedings of SPIE, vol. 3597, pp. 526-531.
- Kollias (1995): The Spectroscopy of Human Melanin Pigmentation, in: Melanin. Its Role in Human Photoprotection, pp. 31-38.
- Matsumoto (2004): Artificial Fingers and Irises: importance of Vulnerability Analysis, at the 7th International Biometrics Conference, 2004, London.
- Thalheim al. (2002): Biometric Access Devices & Programs Put to Test, in: C’t Magazine 11/2002, p. 114. http://www.heise.de/ct/english/02/11/114/
- Pacut, Czajka (2005): Iris Aliveness Detection, at BioSec 2nd Workshop, 2005.

Agenda – Part 2

- State of the art in protecting iris transactions
- Certification programs for iris security
- Statistical evaluation framework
- Countermeasure life cycle

State of the Art

- Various commercially proven liveness detection methods (“countermeasures”) implemented in current Iridian Proof Positive™-certified imagers
- Enrollments always supervised
- Iris images transported to KnoWho® Authentication Server as encrypted and signed Private ID® data packets
- KnoWho database encrypts stored templates
- KnoWho database uses unique IrisCode® template transformations for enhanced privacy

Common Criteria

- Target of evaluation:
  - KnoWho Authentication Server + Panasonic BM-ET100
  - Addressed threats include forged 2-D iris images

- Certified in 2003 to meet assurance level CC EAL 2

Proof Positive™

- Hardware and software certification
- Audits performance, interoperability, safety, security, scalability, usability, reliability
- Includes evaluation of countermeasures effectiveness

Countermeasure Life Cycle

1. Research/prototyping
2. Implementation
3. Tuning
4. Offline test
5. Online test
6. Release decision
7. Circumvention

Confidence-adjusted Error Rates

- Countermeasures development and evaluation at Iridian follows rigorous process
- False-alarm rate (FALR) and penetration rate (PTR) expressed via 95% confidence intervals
- Given K errors in N samples, determine upper bound p_u on the error rate $p = K/N$ with confidence level $\beta = 95\%$

Upper Bound on Error Rate

K	*N*			
	100	200	500	1000
0	3.0 %	1.5 %	0.6 %	0.3 %
1	4.7 %	2.3 %	0.9 %	0.5 %
2	6.2 %	3.1 %	1.3 %	0.6 %
5	10.2 %	5.2 %	2.1 %	1.0 %

$\beta = 95\%$

Minimum Test Set Size

- To validate a specified error rate p_u when K errors have been observed, determine number of samples N_u such that error rate $p = K/N \leq p_u$ with confidence level β = 95%

K	N_u
0	298
1	473
2	627
5	1049

p_u = 1%

iridian® technologies

Countermeasure Life Cycle

1. Research/prototyping	
2. Implementation	
3. Tuning	$FALR < r \cdot FNMR$
4. Offline test	measure *FALRoff*
5. Online test	measure *FALR*, *PTR* confirm *FALRoff*
6. Release decision	if FALR < T_a and PTR < T_p
7. Circumvention	

iridian® technologies

Summary

- Iridian-based iris recognition deployments are protected by proven countermeasures and a secure client-server infrastructure

- As new threats emerge, Iridian and its partners continuously research and develop updated countermeasures

References

- A. J. Mansfield, J. L. Wayman: *Best Practices in Testing and Reporting Performance of Biometric Devices*, Version 2.01, August 2002
- B. D. Jovanovic, P. S. Levy: *A Look at the Rule of Three*, The American Statistician 51(2), May 1997, pp. 137–139
- T. A. Louis: *Confidence Intervals for a Binomial Parameter After Observing No Successes*, The American Statistician 35(3), August 1981, p. 154

Thank you

Bori Toth

boritoth@deloitte.co.uk

+44 7840 389 909

www.deloitte.co.uk/biometrics

Deloitte.

Ulf Cahn von Seelen

ucvs@iridiantech.com

+1 856 222 3155

www.iridiantech.com

iridian®
technologies